(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 887 723 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
30.12.1998 Bulletin 1998/53

(51) Int Cl.[6]: **G06F 1/00**, G06F 12/14

(21) Application number: **98304044.5**

(22) Date of filing: **21.05.1998**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **24.06.1997 US 881139**

(71) Applicant: **INTERNATIONAL BUSINESS MACHINES CORPORATION**
Armonk, NY 10504 (US)

(72) Inventors:
- **Ciacelli, Mark Louis**
  Endicott, New York 13760 (US)
- **Urda, John William**
  Endwell, New York 13760 (US)
- **Lam, Wai Man**
  Mohegan Lake, New York 10547 (US)
- **Kouloheris, Jack Lawrence**
  Ossining, New York 10562 (US)
- **Fetkovich, John Edward**
  Endicott, New York 13760 (US)

(74) Representative: **Boyce, Conor**
IBM United Kingdom Limited,
Intellectual Property Law,
Hursley Park
Winchester, Hampshire SO21 2JN (GB)

(54) Apparatus, method and computer program product for protecting copyright data within a computer system

(57) Apparatus, method and computer program product are provided for digitally processing an encrypted data stream scrambled, for example, according to content scrambling system (CSS) technology. This digital processing insures against communication of clear data within the computer system from a central processing unit (CPU) to any accessible structure, such as memory or a system bus. Descrambling of the (CSS) scrambled data stream occurs within a module executing on the CPU, which is followed by re-encryption of the data prior to transfer from the CPU. By so processing the data, integrity of copyrighted material is maintained, while allowing for software descrambling of the CSS encrypted data stream. Various techniques for establishing the encryption/decryption algorithm pair employed are described. Decryption of the re-encrypted data can occur at a receiving software module and/or a receiving hardware device, such as a decoder.

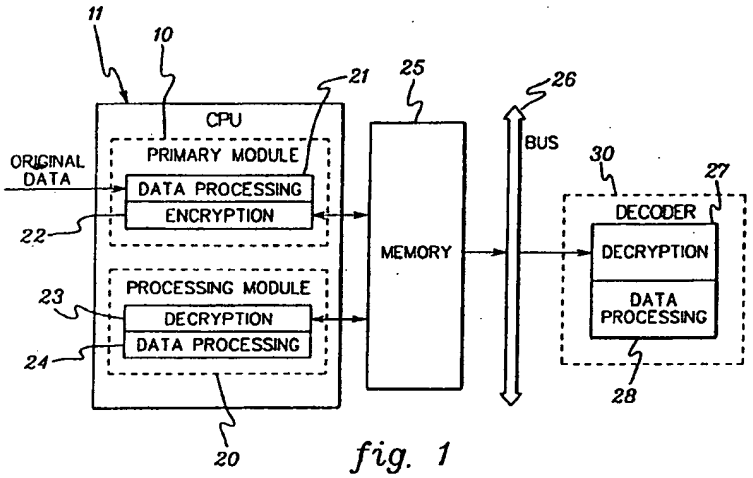

fig. 1

EP 0 887 723 A2

Description

The present invention relates in general to apparatus and method for protecting digital video/audio data and, more particularly, to an apparatus, method and computer program product for encryption/decryption of data within a computer system for communication from a CPU to an accessible internal structure, such as memory or a bus, without exposing the data in unscrambled form at the accessible structure.

Within the past decade, the advent of world-wide electronic communications systems has enhanced the way in which people can send and receive information. In particular, the capabilities of real-time video and audio systems have greatly improved in recent years. In order to provide services such as video-on-demand, video conferencing, and digital video disc (DVD) motion pictures, an enormous amount of bandwidth is required. In fact, bandwidth is often the main inhibitor in the effectiveness of such systems.

In order to overcome the constraints imposed by existing technology, compression systems have emerged. These systems reduce the amount of video and audio data which must be transmitted by removing redundancy in the picture sequence. At the receiving end, the picture sequence is uncompressed and may be displayed in real time.

One example of an emerging video compression standard is the Moving Picture Experts Group ("MPEG") standard. Within the MPEG standard, video compression is defined both within a picture and between pictures. Video compression within a picture is accomplished by conversion of the digital image from the time domain to the frequency domain by a discrete cosine transform, quantization, variable length coding, and Huffman coding. Video compression between pictures is accomplished via a process referred to as "motion estimation", in which a motion vector plus difference data is used to describe the translation of a set of picture elements from one picture to another. The ISO MPEG2 standard specifies only the syntax of bitstream and semantics of the decoding process. The particular choice of coding parameters and tradeoffs in performance versus complexity is left to the system developers.

Digital Versatile Disc (DVD) is an emerging technology which due to its nature, requires extensive encryption in order to protect the data, such as a motion picture, against unauthorized copying.

DVD is a specification for the content of video, audio and other compressed data to be used as playback video, audio and, for example, subtitle data by a DVD decoder. The DVD video data is specified in the Moving Picture Experts Group (MPEG) standard (ISO/IEC 13818-2). As well as being represented by this standard, the data is also encrypted using the industry's Content Scrambling System (CSS), which produces an encrypted, encoded data stream for DVD playback. The data stream can be decrypted by hardware licensed to perform CSS decryption. Conventionally, CSS decryption occurs at a PCI card, which also conventionally includes MPEG decompression of the encrypted, encoded data signal.

The present invention is directed in one particular aspect to improving upon this conventional DVD processing of the encrypted, encoded data stream.

Briefly summarized, this invention comprises in a first aspect apparatus for processing a scrambled data stream within a computer system as claimed in claim 1.

In another aspect, apparatus is provided for processing a data stream within a computer system according to claim 12.

Various enhancements to each of the aspects summarized above are also described and claimed. In addition, corresponding methods and computer program products are presented and claimed.

To restate, in accordance with this invention clear data, whether compressed or uncompressed, is not allowed to be resident in an accessible computer system structure, such as a host memory buffer or system bus to prevent theft of the clear data. The invention is particularly applicable to MPEG encoded and CSS encrypted video data such as employed by digital video disc (DVD) technology. The decryption techniques presented herein allow for subsequent changes, for example, through the flexibility of downloading new microcode, of an encryption/decryption algorithm pair. In addition, the particular scrambling/descrambling algorithm employed may vary. The concept is to initiate the descrambling process by host software, rescramble the data at the central processing unit using a different encryption technique, and then complete the descrambling at the receiving module, whether the receiving module comprises an additional software module executing on the central processing unit or a receiving hardware device, such as a decoder resident on a system bus coupled to the central processing unit. The rescrambling subsequent to primary software descrambling of the received encrypted data may be complete or partial. At the receiving module, the rescrambled data can be decrypted for display, output via an audio card, or undergo further processing.

An embodiment of the invention will now be described with reference to the accompanying drawings, in which:

Fig. 1 depicts one embodiment of a computer system employing encryption/decryption apparatus in accordance with the present invention;

Fig. 2 is a flowchart of one embodiment for accomplishing encryption/decryption processing in accordance with the present invention;

Fig. 3 is a block diagram of one embodiment for updating keys within the encryption and decryption modules and/or devices of an apparatus in accord-

ance with the present invention; and

Fig. 4 is a representation of one embodiment of DVD disc data stream processing using microcode in accordance with the present invention.

Generally stated, the present invention comprises an apparatus, method and computer program product for processing a data stream scrambled, for example, by employing content scrambling system (CSS) technology. As one aspect, the invention comprises descrambling a received CSS encrypted signal at a central processing unit without subsequently exposing a clear copy of the descrambled data in any accessible structure outside the CPU, such as memory or a system bus. This insures that information to be protected, such as security data or copyrighted material (herein collectively referred to as "copyright data"), will not be exposed at a point where illegal copying of the original data stream is feasible (e.g., during data transfer) while still allowing software descrambling of the CSS encrypted stream. In a specific example discussed herein, the encrypted stream might also comprise an encoded stream of video/audio data compressed employing the Moving Picture Experts Group (MPEG) standard (IOS/IEC 13818-2).

In accordance with the present invention, a primary software module within a central processing unit conducts CSS descrambling and then encrypts the data stream using a selected encryption/decryption algorithm before sending any copyright data to a software module and/or hardware device outside the CPU, for example, through memory or a system bus. The external software module and/or hardware device receiving the re-encrypted data stream then decrypts the stream and processes it, e.g., for display in the case of video data or output to an audio card in the case of audio data.

Briefly summarized, the processing involved herein includes determining at the primary software module whether data needs to be protected during subsequent transmission from the computer system's CPU. If "yes", then the primary module communicates to the software module and/or hardware device ultimately to receive the stream of data to establish an encryption/decryption algorithm pair. This communication may involve downloading the decryption algorithm into the receiving software module and/or hardware device or signalling the decrypting software/hardware which decryption algorithm from a plurality of predefined encryption/decryption algorithm pairs is to be used. The primary module uses the selected encryption algorithm to re-encrypt the descrambled data for transfer through any accessible structure, such as memory and/or system buses, to the receiving software module and/or hardware device which is to accomplish the final decryption. The receiving module, which may also be located within the central processing unit, then decrypts the data and performs conventional processing thereon. As an alternative example, the re-encrypted data from the central processing unit may be sent through system memory and/or a system bus to a video decoder for descrambling and then decoding of the data, e.g., for display.

Fig. 1 depicts one embodiment of a computer system to employ apparatus in accordance with the present invention. A primary software module 10 and a secondary (or receiving) processing software module 20 are each executed within the computer system's central processing unit (CPU). A processing unit hardware device 30 (such as a decoder) resides on one of the buses 26 of the computer system. Communication between primary software module 10 and software module 20 and/or processing hardware 30 requires data transfer through memory 25 and/or system bus 26, both located outside the CPU 11. Software module 10 contains a data processing module 21 and an encryption module 22. Data processing module 21 comprises any conventional processing to be done to the data stream, and in accordance with the present invention, also includes descrambling (such as CSS descrambling) of a received encrypted, original data stream. Processing module 20 contains a decryption module 23 and a processing module 24, while processing hardware device 30 includes a decryption device 27 and a data processing device 28.

Original data arrives at the central processing unit 11, for example, from an external storage device or from a computer system network. This data may contain a portion which needs to be protected from illegal copying. This portion is denoted "copyright data" herein to distinguish it from the original data. If the entire original data needs to be protected, then the copyright data is equivalent to the original data. The original data is first transferred to the input of module 10 for processing by data processing 21. Again, for example, this may include descrambling of CSS encrypted original data. The identified copyright data is then re-encrypted by encryption module 22 using a different encryption algorithm, i.e., an encryption algorithm other than CSS encryption. The original data passing through module 10 can comprise an unencrypted data stream or an encrypted data stream. In the first case, processing module 21 processes the original data and encryption module 22 performs an encryption algorithm to encrypt any copyright data. By way of example, the encryption algorithm could be of the type described in B. Schneier, Applied Cryptography, John Wiley & Sons Inc., 2nd Ed. (1996).

In the second case, processing module 21 can decrypt the original data, after which encryption module 22 would re-encrypt the copyright portion of it using a selected encryption algorithm, which again can be of the type described in Applied Cryptography. This procedure is called trans-encryption. Alternatively, processing module 21 can choose not to decrypt the original data and module 22 could then encrypt on top of the originally encrypted copyright data. This procedure is referred to as layer-encryption. Advantageously, trans-encryption allows the encryption algorithm employed within the

computer system in accordance with this invention to be different from that employed by the original data, e.g., CSS encryption. Layer-encryption allows multiple encryption algorithms to be employed, thereby enhancing security.

The encrypted copyright data can be transferred to/through system memory 25 and/or system bus 26 for ultimate receipt by secondary processing module 20 and/or processing hardware device 30. As noted above, module 20 has a decryption module 23 and a data processing module 24, while hardware device 30 contains a decryption device 27 and a data processing device 28. Decryption module 23 and/or device 27 decrypts the data encrypted by encryption module 22. The decrypted data is then processed by the data processing module 24 and/or data processing device 28, respectively.

The encryption/decryption algorithm pair employed by encryption module 22 and decryption module 23 (and/or device 27) can be a default algorithm pair predefined in the design stage of modules 10 & 20 and/or hardware device 30. Alternatively, the algorithm pair can be a downloadable algorithm.

For example, there can be multiple encryption algorithms built into encryption module 22 and multiple decryption modules built into decryption module 23 and/or decryption device 27. Only one matched pair will be used at any given time. Before encryption, the encryption module 22 sends a signal to module 23 and/or device 27 to notice them which particular algorithm module 22 will employ. This signal can be in the form of a software parameter, or a software or a hardware interrupt. The decryption module 23 and/or decryption device 27 then employs the corresponding decryption algorithm of the selected encryption/decryption algorithm pair. Since no actual algorithm content is passed between the modules and devices, the actual encryption algorithm employed will not be known unless reverse engineering is performed within the software modules and/or the hardware devices.

Alternatively, encryption module 22 and decryption module 23 (or decryption device 27) can be predefined at the design stage to include a resident encryption/decryption routine. Before encryption, module 22 would decide on an actual encryption and decryption algorithm pair to be used. Module 22 would use the resident encryption algorithm to encrypt the actual decryption routine of the selected algorithm pair to be used by the decryption module 23 and/or decryption device 27. The encryption module 22 then transmits the encrypted version of the actual decryption algorithm to module 23 and/or device 27. Upon receipt of this information, the decryption module 23 and/or device 27 employs the resident decryption algorithm to decrypt the downloaded decryption algorithm. Module 23 then uses the descrambled decryption algorithm as a procedure call, while device 27 could load the algorithm into a programmable circuit within device 27. After completing downloading of the actual decryption algorithm, module 22 uses the actual encryption algorithm to encrypt the data, and module 23 and/or device 27 employs the downloaded decryption routine to decrypt the data. If an update of the encryption/decryption routine is desired, then a different encryption/decryption algorithm pair is selected and encryption module 22 downloads the corresponding decryption algorithm into the decryption module 23 and/or decryption device 27.

After decryption is performed, the receiving data processing module 24 and/or device 28 performs any required data processing, such as MPEG decoding of a clear, compressed video/audio data signal.

Fig. 2 depicts a flowchart of one embodiment of processing to establish encryption and decryption procedures to secure the data in accordance with the present invention using the apparatus of Fig. 1. This processing flow is started when original data enters the input of software module 10 (Fig. 1). Module 10 initially determines whether the received data needs to be protected 50. If "no", then module 22 communicates the data directly to secondary module 20 and/or device 30 at step 60. For example, in a DVD application, module 10 can examine the Copy Generation Management System (CGMS) data. If the received data needs to be protected, then at step 51 processing communicates from module 22 to decryption module 23 and/or decryption device 27 that decryption is needed prior to use of the data.

Next, processing determines whether a decryption algorithm needs to be downloaded (step 52). If "no", meaning that a default decryption algorithm is to be used, processing proceeds directly to step 54. Otherwise, the algorithm is downloaded into decryption module 23 and/or decryption device 27 at step 53.

After establishing the decryption algorithm, encryption module 22 communicates a key to decryption module 23 and/or decryption device 27 (step 54), and uses the key and the encryption algorithm to encrypt the copyright data (step 55). The encrypted key and encrypted data can be sent as a single bitstream, or separately, to module 23 and/or device 27 by way of system memory and/or a system bus. At step 56, the decryption module 23 and/or decryption device 27 uses the chosen or the downloaded algorithm to decrypt the data. Module 22 then determines whether the encryption key should be updated 57. If "no", the encryption and decryption processing steps 55 & 56 are repeated. If desired, the same encryption key can be used until the end of the data stream transmission. Otherwise, return is made to step 54 for communication of a new encryption key to module 23 and/or device 27.

Fig. 3 depicts one embodiment of apparatus/processing for updating encryption keys pursuant to steps 54 through 57 of Fig. 2. Within module 22 there is a key generation module 79, a key encryption module 80, a data encryption module 81 and a data multiplexer module 82. Key generation module 79 generates an

original key which is encrypted by module 80 and also used by module 81 to encrypt the original data. Data multiplexer 82 combines the encrypted key and the encrypted data into one data stream, which is then transmitted through memory and/or system bus 83 to the decryption module 23 and/or decryption device 27. The decryption module 23 and decryption device 27 contains a data demultiplexer module/device 84, a key decryption module/device 85 and a data decryption module/device 86. The data demultiplexer module/device 84 decouples the received data stream into the encrypted data and the encrypted key. The key is then decrypted by key decryption module/device 85 to produce the original key. Data decryption module 86 uses the original key to decrypt the encrypted data.

Fig. 4 depicts a further embodiment of processing in accordance with the present invention. In this embodiment, rescrambling of the data stream is employed after CSS decryption, along with subsequent descrambling of the re-encrypted stream prior to decompression decoding in a decoder chip. The processings described are preferably accomplished within on-chip microcode.

More particularly, a bit stream is read from a DVD disc 100 into a host processor 110 where a central processing unit conducts DVD descrambling using licensed DVD keys 112. An optional tamper resistance algorithm 114 can be employed to protect the subsequent encryption process. The clear, encoded bit stream is then rescrambled 116 using any available encrypting/decrypting algorithm, i.e., other than CSS encoding. This rescrambled data is delivered to the decoder, for example, an MPEG video decoder 128. Descrambling occurs within decoder 128 subsequent to a microcode load 124 containing the corresponding bit stream descrambling microcode. The exact portions of the stream which are scrambled and then descrambled, as well as the algorithm used, may vary from release to release of the code. The data stream may comprise an MPEG video data stream 118 wherein in one embodiment one or more fields of each picture 120 are scrambled in accordance with bit stream rescramble 116 processing such that the data stream is at least partially re-encrypted subsequent to the DVD descrambling processing 112. A decryption key 122 as well as the microcode load 124 are sent along with the video data stream to bit stream descramble logic 126 within the video decoder 128.

Those skilled in the art will note from the above discussion that in accordance with this invention, clear data (uncompressed or compressed) is never resident in an accessible computer system structure, such as a host memory buffer or system bus, thereby inhibiting theft of the clear data. The invention is particularly applicable to MPEG encoded and CSS encrypted video data such as employed by digital video disc technology. The decryption techniques presented herein allow for subsequent changes, e.g., through the flexibility of new microcode loads, of a decryption algorithm which may have been broken. In addition, the particular scrambling/descrambling algorithm employed by the rescrambling technique of the present invention may vary. The concept is to begin the descrambling process by host software, rescramble the data at the CPU using a different encryption technique, and then complete the descrambling at the receiving module, whether the receiving module comprises an additional software module or a receiving hardware device, such as a decoder. The rescrambling subsequent to primary software descrambling of the received encrypted data may be complete or partial. For example, in one embodiment, certain MPEG data can be scrambled by the host software. The host would then transmit the appropriate descrambling microcode loads or a single microcode load with an appropriate key or keys to the receiving module or receiving hardware device. At the receive module, the microcode performs the inverse of the scrambling algorithm, used by the host. The key may be static or accumulated.

Further, those skilled in the art will note that the present invention can be included in an article of manufacture (e.g., one or more computer program products) having, for instance, computer useable media. The media has embodied therein, for instance, computer readable program code means for providing and facilitating the capabilities of the present invention. The articles manufactured can be included as part of the computer system or sold separately.

The flow diagrams depicted herein are provided by way of example. For instance, in certain cases the steps may be performed in differing order, or steps may be added, deleted or modified. Further, although described principally herein with reference to a single primary module, a single receiving processing module, and a single processing hardware device, multiple modules and devices of each type may be employed as apparatus in accordance with the present invention.

Claims

1. Apparatus for processing a scrambled data stream within a computer system having a central processing unit (CPU) coupled to receive the scrambled data stream, comprising:

   descrambling means within the central processing unit for descrambling the received, scrambled data stream to produce a clear data stream;

   re-encryption means within the central processing unit for re-encrypting the clear data stream to produce an encrypted data stream, wherein said scrambled data stream is produced from a different encryption algorithm than said encrypted data stream;

   means for transferring the encrypted data

stream from the central processing unit to a second structure of the computer system, said second structure being coupled to the CPU; and

decryption means coupled to the second structure for receiving the encrypted data stream therefrom and for decrypting the encrypted data stream to produce said clear data stream, wherein said clear data stream is unexposed when transferred from the central processing unit to said second structure coupled to the CPU, while said descrambling means within the central processing unit accomplishes descrambling of the received scrambled data stream.

2. The apparatus of claim 1, wherein said scrambled data stream comprises a scrambled, encoded data stream and wherein said apparatus further comprises a decoder coupled to said decryption means for decoding a clear, encoded data stream produced by said decryption means.

3. The apparatus of claim 2, wherein said clear, encoded data stream comprises a video data stream and wherein said decoder comprises an MPEG video decoder.

4. The apparatus of claim 2, wherein said scrambled, encoded data stream comprises a CSS scrambled, MPEG encoded data stream, and wherein said descrambling means comprises means for CSS descrambling the scrambled, encoded data stream within the CPU and said decoder comprises means for MPEG decoding said clear, encoded data stream.

5. The apparatus of claim 2, wherein said decoder comprises a decoding hardware device and said decryption means resides within said decoding hardware device.

6. The apparatus of claim 1, wherein said re-encryption means further comprises means for providing a key for use in re-encrypting the clear data stream, and wherein said decryption means includes means for employing the key in decrypting the encrypted data stream.

7. The apparatus of claim 6, wherein said re-encryption means further comprises means for encrypting said key to produce an encrypted key, and for multiplexing the encrypted key and the encrypted data stream into a multiplexed data stream for transfer to said second structure coupled to the CPU, and wherein said decryption means further comprises means for demultiplexing said multiplexed data stream to obtain said encrypted key and said encrypted data stream, and wherein said decryption means further comprises means for decrypting said encrypted key.

8. The apparatus of claim 1, further comprising means for selecting an encryption/decryption algorithm pair for-use by said re-encryption means and said decryption means.

9. The apparatus of claim 8, wherein said means for selecting comprises means for downloading a decryption algorithm of said selected encryption/decryption algorithm pair from said re-encryption means to said decryption means, said means for downloading including means for encrypting the decryption algorithm for transfer between the re-encryption means and the decryption means.

10. The apparatus of claim 8, wherein said means for selecting comprises means for selecting said encryption/decryption algorithm pair from a plurality of encryption/decryption algorithm pairs at said re-encryption means and said decryption means, and wherein said means for selecting comprises means for noticing the decryption means which decryption algorithm of said plurality of encryption/decryption algorithm pairs corresponds with an encryption algorithm employed by said re-encryption means.

11. The apparatus of claim 1, wherein said decryption means comprises a decryption module disposed within the central processing unit, and said second structure coupled to the CPU comprises memory.

12. Apparatus for processing a data stream within a computer system having a central processing unit (CPU) coupled to receive the data stream, said apparatus comprising:

encryption means within the CPU for encrypting identified copyright data within the data stream to produce therefrom encrypted data;

means for transferring the encrypted data from the central processing unit to a structure of the computer system coupled thereto, wherein said copyright data is only transferred from the central processing unit as said encrypted data; and

decryption means coupled to said structure receiving the encrypted data, said decryption means comprising means for decrypting the encrypted data.

13. The apparatus of claim 12, further comprising means for identifying within the central processing unit said copyright data of the data stream, said means for identifying providing said identified cop-

yright data to said encryption means.

14. The apparatus of claim 13, wherein the data stream comprises a scrambled, encoded data stream, and wherein said apparatus further comprises descrambling means for descrambling the scrambled, encoded data stream within the central processing unit to produce a clear, encoded data stream, and wherein said means for identifying comprises means for examining the clear, encoded data stream to identify copyright data for encryption by said encryption means.

15. The apparatus of claim 12, wherein said decryption means comprises a microcode decryption device.

16. The apparatus of claim 12, wherein said data stream comprises a scrambled data stream, and wherein said apparatus further comprises means for descrambling the scrambled data stream prior to said encrypting of the identified copyright data by said encryption means, wherein said scrambled data stream is produced from a different encryption algorithm than said encrypted data produced by said encryption means.

17. The apparatus of claim 12, wherein said encryption means further comprises means for providing a key for use in said encrypting of the identified copyright data and for use by said decryption means for decrypting the encrypted data.

18. The apparatus of claim 17, wherein said encryption means further comprises means for encrypting said key to produce an encrypted key, and for multiplexing the encrypted key and the encrypted data into a multiplexed data stream for transfer to said structure coupled to the CPU, and wherein said decryption means further comprises means for demultiplexing said multiplexed data stream to obtain said encrypted key and said encrypted data, and wherein said decryption means further comprises means for decrypting said encrypted key.

19. The apparatus of claim 12, further comprising means for selecting an encryption/decryption algorithm pair for use by said encryption means and said decryption means from a plurality of predefined encryption/decryption algorithm pairs, said selected encryption/decryption algorithm pair comprising an encryption algorithm and a corresponding decryption algorithm, said encryption algorithm being employed by said encryption means, and said corresponding decryption algorithm being employed by said decryption means.

20. A method for processing a scrambled data stream within a computer system having a central processing unit and a structure coupled thereto, said method comprising:

(a) receiving the scrambled data stream at the central processing unit (CPU);

(b) descrambling the scrambled data stream within a module executing on the central processing unit to produce clear data;

(c) re-encrypting the clear data within the central processing unit, said re-encrypting producing at least partially encrypted data;

(d) subsequent to said re-encrypting, transferring the at least partially encrypted data from the central processing unit to a second structure of the computer system, said second structure being coupled to the central processing unit; and

(e) subsequent to said transferring, retrieving and decrypting the at least partially encrypted data to produce clear data, wherein said clear data is unexposed when transferred from the central processing unit to the structure coupled thereto, while said descrambling occurs within the module executing on the central processing unit, and wherein the scrambled data stream is produced from a different encryption algorithm than employed by said re-encrypting (c) to produce said at least partially encrypted data.

21. A computer program producing comprising a computer usable medium having computer readable program code means therein for use in processing a scrambled data stream within a computer system having a central processing unit and a structure coupled thereto, said computer readable program code means in said computer program product comprising:

computer readable program code means for causing a computer to affect receiving of the scrambled data stream at the central processing unit and for descrambling the scrambled data stream within the central processing unit to produce clear data, and for re-encrypting the clear data within the central processing unit to produce at least partially encrypted data;

computer readable program code means for causing a computer to affect transferring of said at least partially encrypted data from the central processing unit to the structure coupled thereto; and

computer readable program code means for

causing a computer to affect retrieving of the at least partially encrypted data from the structure coupled to the CPU and for decrypting the at least partially encrypted data, said decrypting producing clear data, wherein said clear data is unexposed when transferred from the central processing unit to the structure coupled thereto, while said descrambling occurs within the central processing unit.

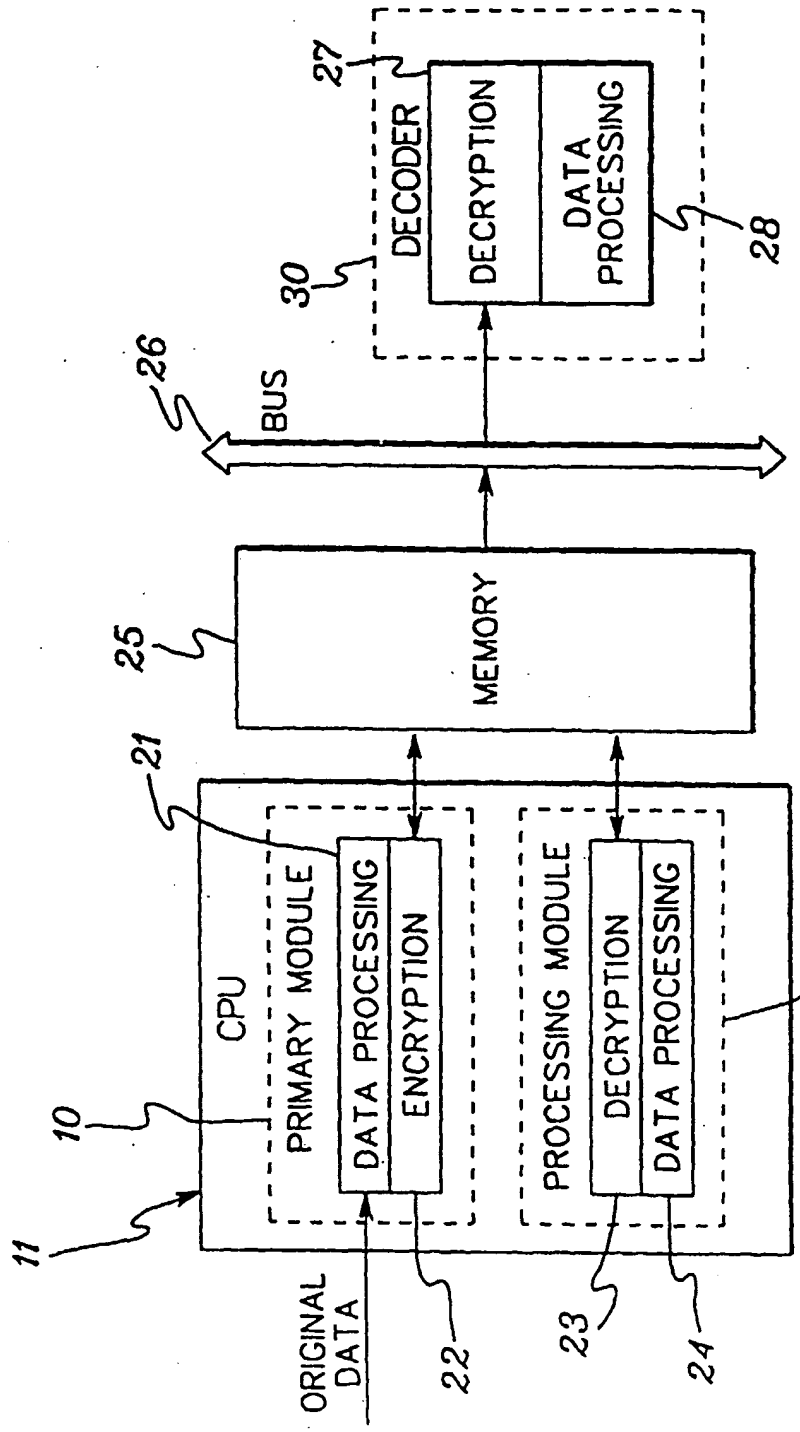
27
DECODER
DECRYPTION
DATA PROCESSING
28
30
26
BUS
25
MEMORY
21
CPU
PRIMARY MODULE
DATA PROCESSING
ENCRYPTION
PROCESSING MODULE
DECRYPTION
DATA PROCESSING
20
10
11
ORIGINAL DATA
22
23
24

fig. 1

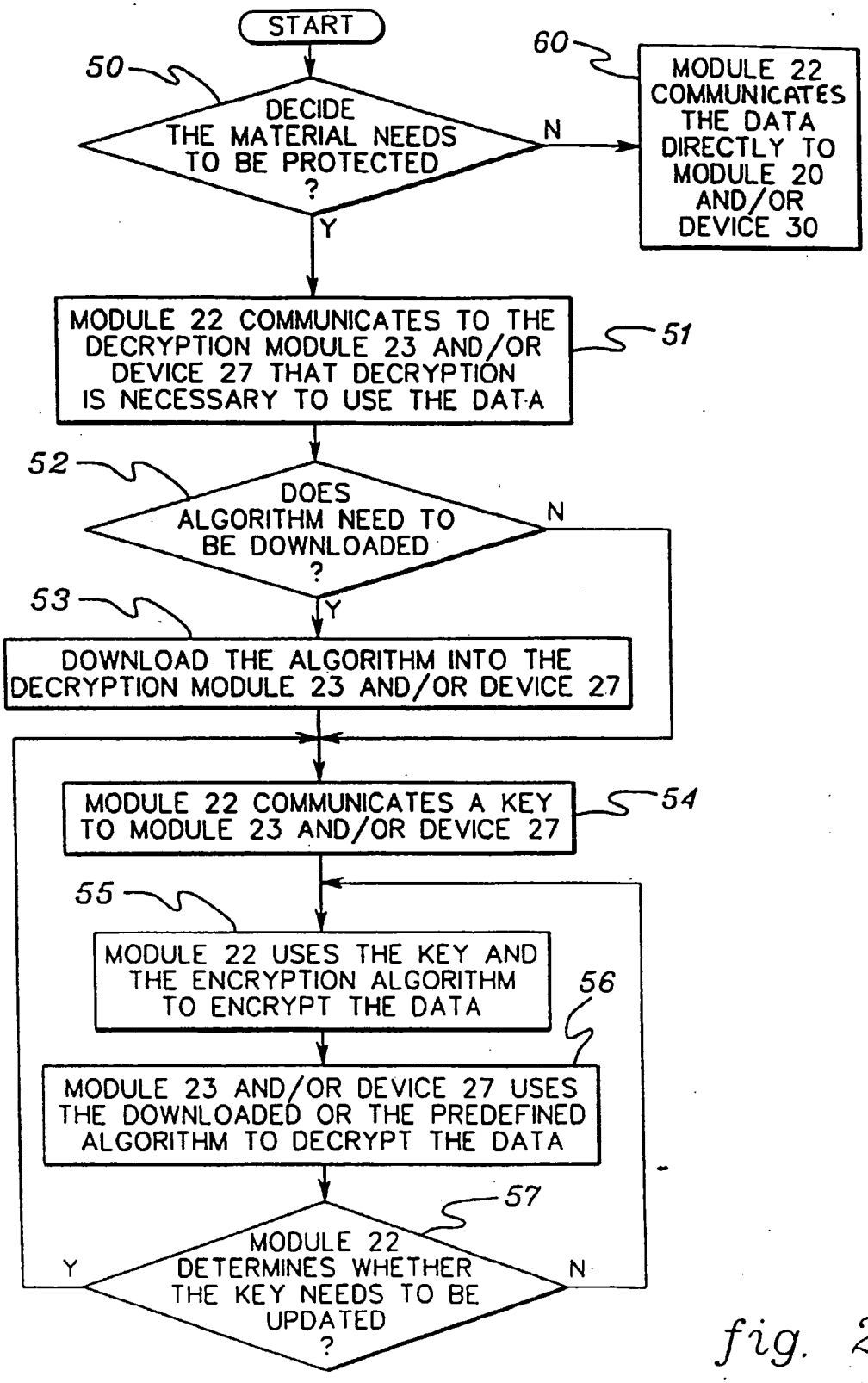
START
50
DECIDE THE MATERIAL NEEDS TO BE PROTECTED ?
N
60
MODULE 22 COMMUNICATES THE DATA DIRECTLY TO MODULE 20 AND/OR DEVICE 30
Y
MODULE 22 COMMUNICATES TO THE DECRYPTION MODULE 23 AND/OR DEVICE 27 THAT DECRYPTION IS NECESSARY TO USE THE DATA
51
52
DOES ALGORITHM NEED TO BE DOWNLOADED ?
N
Y
53
DOWNLOAD THE ALGORITHM INTO THE DECRYPTION MODULE 23 AND/OR DEVICE 27
MODULE 22 COMMUNICATES A KEY TO MODULE 23 AND/OR DEVICE 27
54
55
MODULE 22 USES THE KEY AND THE ENCRYPTION ALGORITHM TO ENCRYPT THE DATA
56
MODULE 23 AND/OR DEVICE 27 USES THE DOWNLOADED OR THE PREDEFINED ALGORITHM TO DECRYPT THE DATA
57
MODULE 22 DETERMINES WHETHER THE KEY NEEDS TO BE UPDATED ?
Y
N

fig. 2

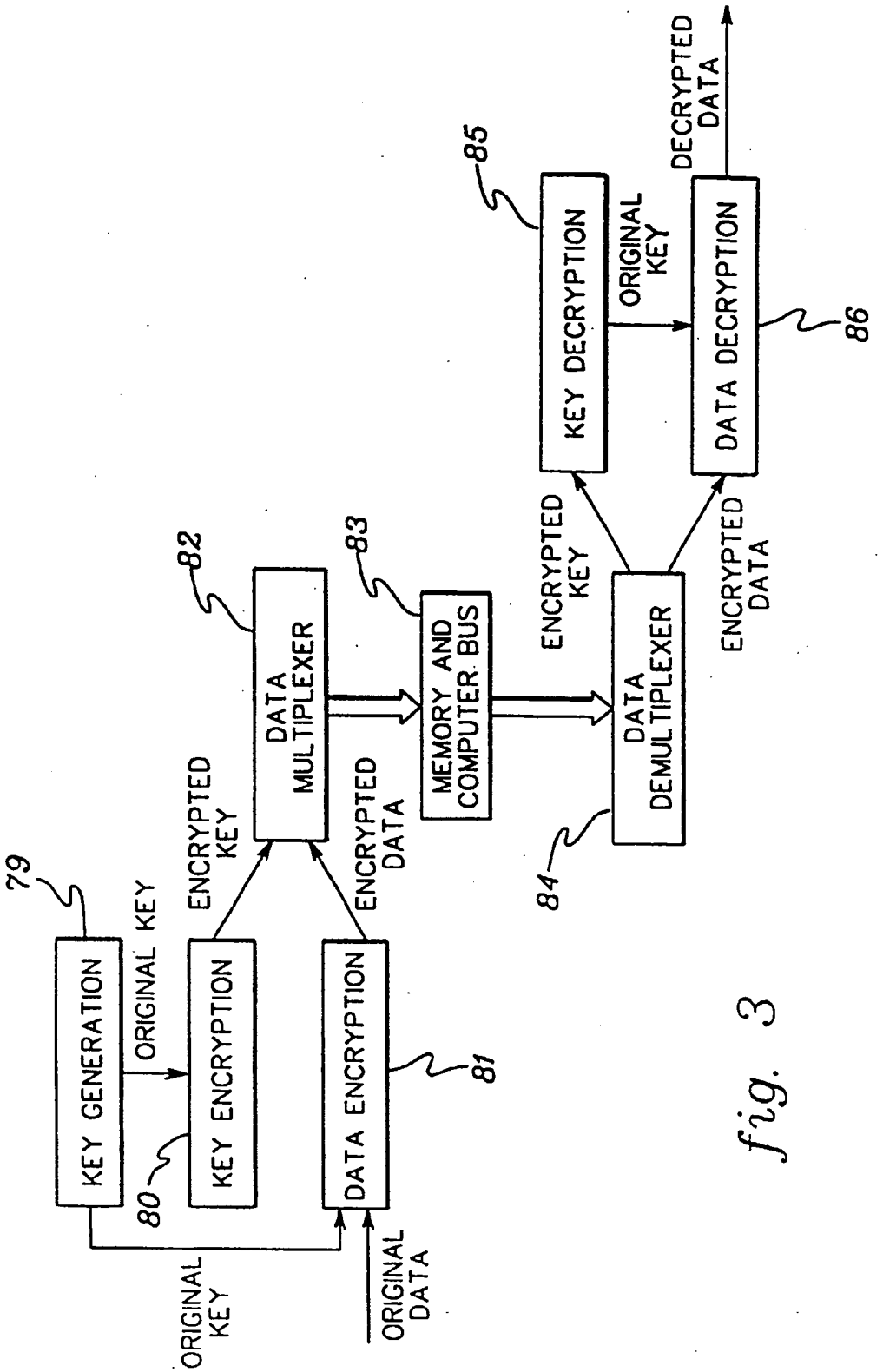
KEY GENERATION
79
ORIGINAL KEY
KEY ENCRYPTION
80
ENCRYPTED KEY
DATA ENCRYPTION
81
ENCRYPTED DATA
ORIGINAL KEY
ORIGINAL DATA
DATA MULTIPLEXER
82
MEMORY AND COMPUTER BUS
83
DATA DEMULTIPLEXER
84
ENCRYPTED KEY
ENCRYPTED DATA
KEY DECRYPTION
85
ORIGINAL KEY
DATA DECRYPTION
86
DECRYPTED DATA

fig. 3

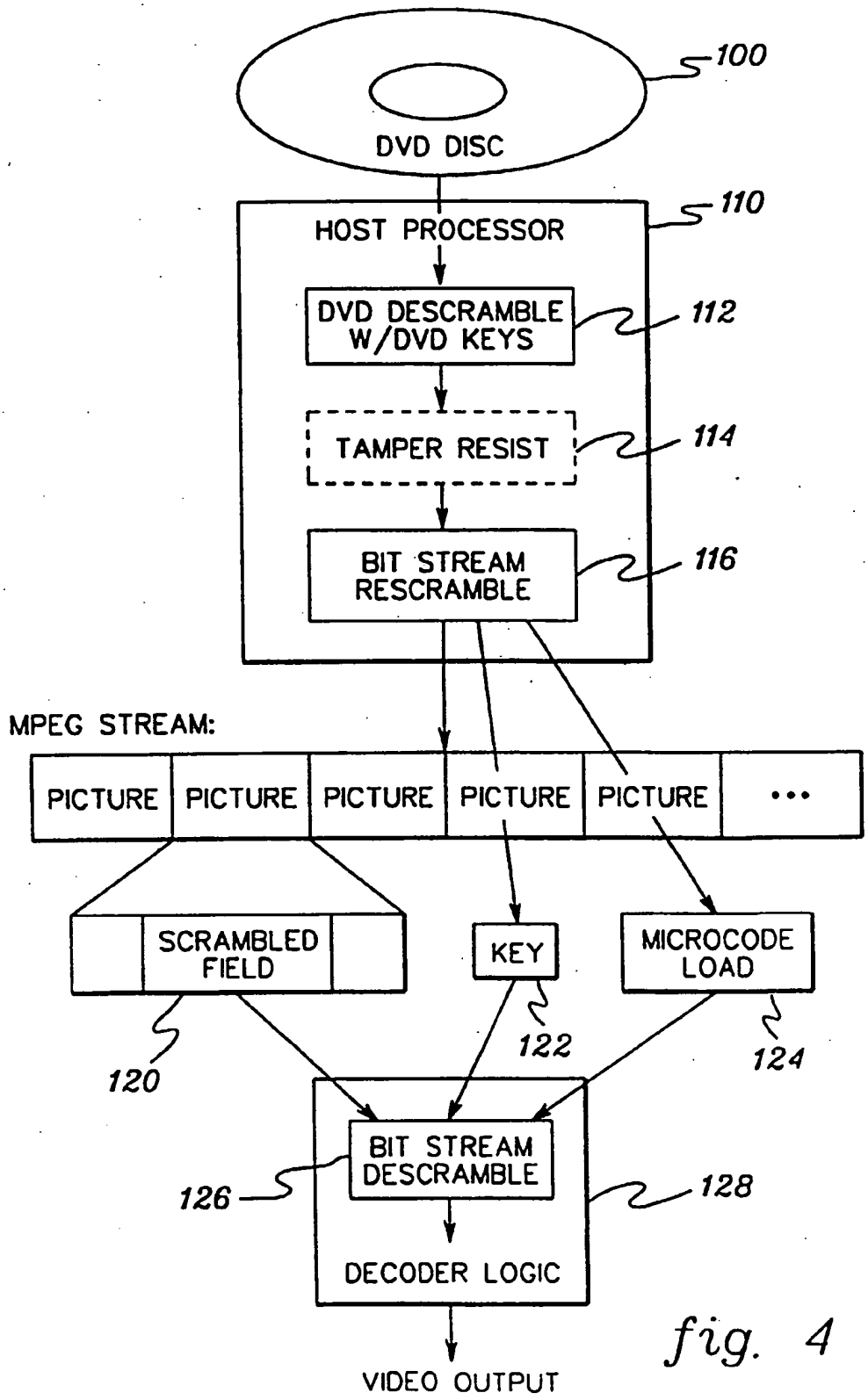
100
DVD DISC
110
HOST PROCESSOR
DVD DESCRAMBLE W/DVD KEYS
112
TAMPER RESIST
114
BIT STREAM RESCRAMBLE
116
MPEG STREAM:
PICTURE
PICTURE
PICTURE
PICTURE
PICTURE
...
SCRAMBLED FIELD
KEY
MICROCODE LOAD
120
122
124
BIT STREAM DESCRAMBLE
126
128
DECODER LOGIC
VIDEO OUTPUT

fig. 4

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 887 723 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
01.08.2007 Bulletin 2007/31

(43) Date of publication A2:
30.12.1998 Bulletin 1998/53

(21) Application number: **98304044.5**

(22) Date of filing: **21.05.1998**

(51) Int Cl.:
G06F 1/00 (2006.01) *G06F 12/14* (2006.01)

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **24.06.1997 US 881139**

(71) Applicant: **International Business Machines Corporation**
Armonk, NY 10504 (US)

(72) Inventors:
- **Ciacelli, Mark Louis**
  Endicott,
  New York 13760 (US)
- **Urda, John William**
  Endwell,
  New York 13760 (US)
- **Lam, Wai Man**
  Mohegan Lake,
  New York 10547 (US)
- **Kouloheris, Jack Lawrence**
  Ossining,
  New York 10562 (US)
- **Fetkovich, John Edward**
  Endicott,
  New York 13760 (US)

(74) Representative: **Boyce, Conor**
IBM United Kingdom Limited,
Intellectual Property Law,
Hursley Park
Winchester,
Hampshire SO21 2JN (GB)

(54) Apparatus, method and computer program product for protecting copyright data within a computer system

(57) Apparatus, method and computer program product are provided for digitally processing an encrypted data stream scrambled, for example, according to content scrambling system (CSS) technology. This digital processing insures against communication of clear data within the computer system from a central processing unit (CPU) to any accessible structure, such as memory or a system bus. Descrambling of the (CSS) scrambled data stream occurs within a module executing on the CPU, which is followed by re-encryption of the data prior to transfer from the CPU. By so processing the data, integrity of copyrighted material is maintained, while allowing for software descrambling of the CSS encrypted data stream. Various techniques for establishing the encryption/decryption algorithm pair employed are described. Decryption of the re-encrypted data can occur at a receiving software module and/or a receiving hardware device, such as a decoder.

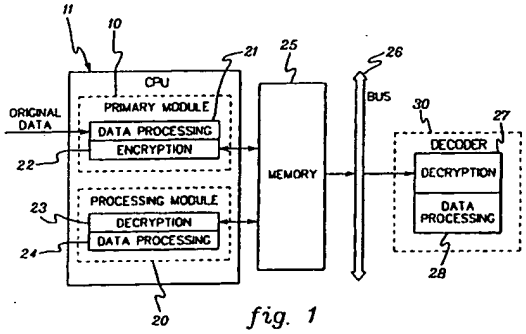

fig. 1

EP 0 887 723 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 30 4044

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	EP 0 715 241 A2 (MITSUBISHI CORP [JP]) 5 June 1996 (1996-06-05) * claim 7; figures 3,5 * * column 3, lines 7-27 * * column 6, lines 41-44 * * column 9, line 57 - column 10, line 29 * * column 10, lines 48-59 * * column 11, lines 6-21 * * column 11, lines 43-46 * * column 13, lines 12-39 * * column 14, line 54 - column 15, line 33 * * column 16, line 57 - column 17, line 2 * * column 22, lines 46-51 * * column 23, lines 25-34 * * column 26, lines 6-13 * * column 28, lines 20-35 *	1-5,11, 20,21	INV. G06F1/00 G06F12/14
X A	US 5 138 659 A (KELKAR KRIS [US] ET AL) 11 August 1992 (1992-08-11) * figures 1-3 * * column 2, lines 13-36 * * column 2, lines 47-50 * * column 2, line 56 - column 3, line 3 * * column 3, lines 11-18 * * column 3, line 52 - column 4, line 57 * * column 5, lines 15-31 * * column 6, lines 37-52 *	1 2-5,11, 20,21	TECHNICAL FIELDS SEARCHED (IPC) G06F H04L H04N G11B
A	WO 96/06504 A (THOMSON CONSUMER ELECTRONICS [US]; CHANEY JOHN WILLIAM [US]) 29 February 1996 (1996-02-29) * page 3, line 3 - page 4, line 5 * * page 10, lines 13-21 * * page 14, lines 23-25 *	1-5,11, 20,21	

-/--

~~The present search report has been drawn up for all claims~~

Place of search	Date of completion of the search	Examiner
Munich	12 March 2007	Preuss, Norbert

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 30 4044

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	WO 96/03835 A2 (MACROVISION CORP [US]) 8 February 1996 (1996-02-08) * page 8, lines 12-35 * * page 14, lines 17-37 *	1-5,11, 20,21	
A	GIACHETTI J-L ET AL: "A COMMON CONDITIONAL ACCESS INTERFACE FOR DIGITAL VIDEO BROADCASTING DECODERS" IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, IEEE SERVICE CENTER, NEW YORK, NY, US, vol. 41, no. 3, August 1995 (1995-08), pages 836-841, XP000539543 ISSN: 0098-3063 * pages 1-2 *		TECHNICAL FIELDS SEARCHED (IPC)

~~The present search report has been drawn up for all claims~~

Place of search	Date of completion of the search	Examiner
Munich	12 March 2007	Preuss, Norbert

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

Application Number
EP 98 30 4044

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing more than ten claims.

☐ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims and for those claims for which claims fees have been paid, namely claim(s):

☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

☐ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.

☐ As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.

☐ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:

☒ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:

1-5, 11, 20, 21

European Patent Office

LACK OF UNITY OF INVENTION
SHEET B

Application Number
EP 98 30 4044

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. claims: 1-5,11,20,21

   Apparatus, method and computer program to receive scrambled or encrypted data, descramble, reencrypt with different algorithm, send encrypted data to second structure, second structure decrypting data to produce clear data again.

   ---

2. claims: 12-14,16

   Apparatus identifying copyright data

   ---

3. claims: 6-7,17-18

   Apparatus to securely transfer cryptographic keys from a first to a second part

   ---

4. claims: 8-10,19

   Apparatus to select and securely communicate cryptographic algorithms

   ---

5. claim: 15

   Microcode decryption device

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 30 4044

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

12-03-2007

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0715241 A2	05-06-1996	DE 69532434 D1	19-02-2004
		DE 69532434 T2	11-11-2004
US 5138659 A	11-08-1992	AU 645943 B2	27-01-1994
		AU 1595892 A	05-11-1992
		BR 9201658 A	15-12-1992
		CA 2067445 A1	03-11-1992
		DE 69221199 D1	04-09-1997
		DE 69221199 T2	29-01-1998
		EP 0512398 A2	11-11-1992
		JP 2717238 B2	18-02-1998
		JP 5183885 A	23-07-1993
WO 9606504 A	29-02-1996	AT 208979 T	15-11-2001
		AU 3238595 A	22-03-1996
		AU 701593 B2	04-02-1999
		AU 3239495 A	14-03-1996
		BR 9508621 A	30-09-1997
		BR 9508622 A	19-05-1998
		CA 2196406 A1	07-03-1996
		CA 2196407 A1	29-02-1996
		CN 1158202 A	27-08-1997
		CN 1158203 A	27-08-1997
		DE 69514843 D1	02-03-2000
		DE 69514843 T2	18-05-2000
		DE 69523937 D1	20-12-2001
		DE 69523937 T2	06-06-2002
		EP 0878088 A2	18-11-1998
		EP 0782807 A1	09-07-1997
		ES 2141371 T3	16-03-2000
		ES 2162935 T3	16-01-2002
		FI 970677 A	18-02-1997
		HK 1002482 A1	21-03-2003
		HK 1002483 A1	29-10-2004
		IN 184151 A1	24-06-2000
		JP 3411581 B2	03-06-2003
		JP 10506507 T	23-06-1998
		JP 10505720 T	02-06-1998
		JP 3202241 B2	27-08-2001
		PL 318647 A1	07-07-1997
		PT 782807 T	31-05-2002
		RU 2184392 C2	27-06-2002
		TW 395107 B	21-06-2000
		WO 9607267 A2	07-03-1996
WO 9603835 A2	08-02-1996	AT 193630 T	15-06-2000

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 30 4044

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

12-03-2007

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9603835 A2		AU 697727 B2	15-10-1998
		AU 3127695 A	22-02-1996
		BR 9508340 A	09-09-1997
		CA 2195939 A1	08-02-1996
		CN 1159272 A	10-09-1997
		DE 69517324 D1	06-07-2000
		DE 69517324 T2	14-12-2000
		DK 775418 T3	13-11-2000
		EP 0775418 A2	28-05-1997
		HK 1001301 A1	05-03-2004
		JP 3217068 B2	09-10-2001
		JP 10503338 T	24-03-1998
		NZ 290521 A	28-10-1998
		US 5574787 A	12-11-1996

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82